UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,135	11/14/2001	David Carroll Challener	RSP9 2001 0049	6172

53493 7590 10/05/2005

LENOVO (SINGAPORE) PTE. LTD.
BUILDING 675, MAIL C-137
4401 SILICON DRIVE
DURHAM, NC 27709

EXAMINER	
LASHLEY, LAUREL L	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 10/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/993,135	CHALLENER ET AL.	
	Examiner	Art Unit	
	Laurel Lashley	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 38 have been examined.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 14 November 2001 was filed the application. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Drawings

3. The drawings were received on 15 February 2002. These drawings are acceptable.

Specification

4. The specification is objected to because of the following informality:

- Incomprehensible sentence (*see page 3 of 42, lines 23-24; should be --he-- instead of* "the").

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 1 – 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Shimizu et al. in US Patent 6,085,323 (hereinafter '323)*, and further in view of *Godoroja et al. in US Patent 6,032,258 (hereinafter '258).*

As it relates to claim 1, *Shimizu et al. in US '323 teaches*:

A method for providing access to secure data through a portable computing system during a specified time, wherein said method comprises:

establishing a connection (*see US '323: column 2, line 47: where a signal exchange is possible between apparatuses*) between said portable computing system (*see column 2, line 44: first information processing apparatus*) and a base computing system (*see column 2, line 45; second information processing apparatus*) to provide for transfer of data between said portable computing system and said base computing system;

but does not teach

verifying identity of said base computing system within said portable computing system;

resetting a timer within said portable computing system to run for a specified time; and

providing access to said secure data only when said timer is running.

Godoroja et al. in US '258 however, does teach

verifying identity of said base computing system within said portable computing system (*see US '258: column 3, lines 15 – 21: where it is inherent*

that a nodes (instance case: PCS and BCS) each have a clock mechanism with correlating time which is an indicator of a valid identity);

resetting a timer within said portable computing system to run for a specified time (*see column 3, lines 15 – 16: where each node maintains a time reference*) ; and

providing access to said secure data only when said timer is running (see column 6, lines 15 – 16: where all data transmissions have time reference, if not it is considered invalid).

For claim 1, *it would be obvious to one of ordinary skill in the art at the time of the invention to modify the methods of Godoroja et al. and Shimizu et al. as they both use features of a portable and base computing systems and timer functionalities within the same field of endeavor (connecting to and accessing secure data during specified time) and with the same problem sought to be solved (verifying that the rightful users are in possession of computer systems before features are enabled within a time measure).*

For claim 2, *Shimizu et al in US '323 teaches*

receiving and storing a public cryptographic key from said base computing system during an initialization process,

following said initialization process, generating a random number within said portable computing system;

transmitting said random number to said base computing system;

receiving a number transmitted from said base computing system; decrypting

said number transmitted from said base computing system to form a decrypted number; and

determining that said decrypted number matches said random number *(see column 2, lines 49 – 65).*

For claim 3, *Shimizu et al. in US '323 teaches*

whether a password is entered correctly in said portable computing *as taught by system (see column 13, line 44: authentication of a password).*

For claim 4, *Godoroja et al. teaches*

transmitting an initial password to said base computing system during an initialization process,

storing said initial password within said base computing system;

following said initialization process, transmitting a present password to said base computing system;

determining in said base computing system that said initial password matches said present password;

transmitting an approval code from said base computing system to said portable computing system; and

determining that said approval code has been received (*US '258: see column 6, lines 59 – 60: where verification is determined because only the source and destination nodes know the password*).

For claim 5, *Shimizu et al. in US '323 teaches*

wherein said connection is established through a switched telephone network (*US '323: see column 15, line 13: wherein a network can encompass applicant's network*).

For claim 6, *Godoroja et al. in US '258 teaches*

wherein

said timer includes a timer register storing a number corresponding to a time remaining (*US '258: see column 3, lines 5 –6: clock mechanism*),

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register (*US '258: column 4, lines 61 – 65*).

As it relates to claim 7, *Shimizu et al. in US '323 teaches*:

A method providing for access to secure data through a portable computing system, wherein said access to said secure data is limited to a specified time, and wherein said method comprises:

initializing a base computing system and said portable computing system to work together as a system by an initialization process comprising storing data identifying said base computing system within said portable computing system (*US '323: see column 2; line 67 and column 3, lines 1 –2*); and

resetting said portable computing system by a reset process following said initialization process including:

establishing a connection to transmit data between said portable computing system and a base computing system (*column 3, lines 3 –4*);

determining, using said data identifying said base computing system, that said connection has been made between said portable computing system and said base computing system (*column 3, line 7, correlation storage means*);

but does not teach

setting a timer within said portable computing system to run until said specified time has expired;

determining if said timer is running; and providing access to said secure data only when said timer is running.

Godoroja et al. in US '258 however does teach

setting a timer within said portable computing system to run until said specified time has expired (*US '258: see column 3, lines 23 – 24: clock synchronization*);

determining if said timer is running; and providing access to said secure data only when said timer is running (*see column 5, lines 58 – 65*).

For claim 7, *it would be obvious to one of ordinary skill in the art at the time of the invention to modify the methods of Shimizu et al. and Godoroja et al. as they both use features of a portable and base computing systems and timer functionalities within the same field of endeavor (connecting to and accessing secure data during specified time) and with the same problem sought to be solved (verifying that the rightful users are in possession of computer systems before features are enabled within a time measure).*

For claim 8, *Godoroja et al in US '258 teaches*

wherein

said initialization process additionally includes determining whether said data identifying a base computing system has been previously stored in said portable computing system;

if said data identifying a base computing system is determined to have been previously stored, said data identifying a base computing system remains without being overwritten during said initialization process (*US 258: see column 2, lines 18 – 23: where instance deemed "old" by time reference then packet is discarded whereby it is inherent that a previously stored instance is retained without modification/replacement i.e. being overwritten*).

For claim 9, *Shimizu et al. in US '323 teaches*

The method of claim 8, wherein said data identifying said base computing is a public cryptographic key of said base computing system, and wherein said process of determining that said connection has been made between said portable computing system and said base computing system includes:

generating and storing random number within said portable computing system;

transmitting said random number from said portable computing system to said base computing system;

encrypting said random number within said base computing system with a private cryptographic key of said base computing system to form an encrypted number;

transmitting said encrypted number from said base computing system to said portable computing system; (*US '323: see column 3, lines 6 – 12*)

decrypting said encrypted number within said portable computing system with said public cryptographic key of said base computing system to form a decrypted number; (*see column 3, lines 13 – 24*) and

but does not teach

comparing said decrypted number with said random number stored within said portable computing system.

Godoroja et al. in US '258 however does teach

comparing said decrypted number with said random number stored within said portable computing system (*US '258: column 4, line 61: as performed by the comparison step*) *as taught by Godoroja et al. in US '258.*

For claim 9, *it would be obvious to one of ordinary skill in the art at the time of the invention to modify the methods of Godoroja et al. and Shimizu et al. as they both use features of a portable and base computing systems and timer functionalities within the same field of endeavor (identifying and verifying public cryptographic key of computing systems) and with the same problem sought to be solved (secure connections between computer systems).*

For claim 10, *Godoroja et al in US '258 teaches*

wherein

said timer includes a timer register storing a number corresponding to a time remaining (*US '258: see column 3, lines 5 – 6*),

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register (*see column 4, lines 61 –65*).

For claim 11, *Godoroja et al. in US '258 teaches*

wherein

said method additionally comprises receiving an input corresponding to a time, and

setting said specified time according to said input *(US '258: see column 3, lines 42 – 45) as taught by*

For claim 12, *Shimizu et al. in US '323 teaches*

additionally comprising storing a cryptographic public cryptographic key of said portable computing system within said base computer system (*US '323: column 3, line 36 – 40*).

For claim 13, *Godoroja et al (US '258) teaches*

said initialization process additionally includes receiving a present password as an input, determining if a password has been previously stored, and storing said present password in response to a determination that said password has not been previously stored, and

said reset process additionally includes receiving a present password as an input and determining if said password matches a stored password;

said timer is set within said portable computing system only in response to a determination that said password matches said stored password (*US '258: column 3, lines 30 – 41*).

For claim 14, *Godoroja et al. (US '258) teaches*

wherein

said present password is received as an input within said portable computing system,

said present password is transmitted from said portable computing system to said base computing system,

said present password is stored within said base computing system following a determination that a password is not previously stored within said base computing system;

a determination is made in said base computing system of whether said present password matches a stored password, (*US '258: see column 3, lines 30 – 41*)

said reset process additionally includes transmitting an approval code from said base computing system to said portable computing system in response to a determination that said present password matches said stored password, and

said timer is set within said portable computing system in response to receiving said approval code (*US '258: see column 6, lines 59 – 60*).

For claim 15, *Shimizu et al. in US '323 teaches*

The method of claim 14, wherein said data identifying said base computing is a public cryptographic key of said base computing system, and wherein said process of

determining that said connection has been made between said portable computing system and said base computing system includes:

generating and storing random number within said portable computing system;

concatenating said random number and said present password within said portable computing system to form a concatenated number;

encrypting said concatenated number within said portable computing system with said public cryptographic key of said base computing system to form a first encrypted number;

transmitting said first encrypted number from said portable computing system to said base computing system; (*US '323: see column 3, lines 6 – 12*)

decrypting said first encrypted number within said base computing system with a private cryptographic key of said base computing system to form a decrypted number;

dividing said decrypted number to form a decrypted random number and said present password;

encrypting said decrypted random number within said base computing system with a private cryptographic key of said base computing system to form a second encrypted number;

transmitting said second encrypted number from said base computing system to said portable computing system;

decrypting said second encrypted number within said portable computing system with said public cryptographic key of said base computing system to form a decrypted number; (*see column 3, lines 13 – 24*) and

but does not teach

comparing said decrypted number with said random number stored within said portable computing system.

Godoroja et al. in US '258 however teaches

comparing said decrypted number with said random number stored within said portable computing system (*US '258: see column 4, line 61*) *as taught by Godoroja et al.*

For claim 15, *it would be obvious to one of ordinary skill in the art at the time of the invention to modify the methods of Shimizu et al. and Godoroja et al. as they both use features of a portable and base computing systems and timer functionalities within the same field of endeavor (identifying and verifying public cryptographic key of computing systems) and with the same problem sought to be solved (secure connections between computer systems).*

For claim 16, *Shimizu et al in US '323 teaches*

A system for providing controlled access to secure data, wherein said system comprises:

a portable computing system providing said controlled access to secure data during a specified time, wherein said portable computing system includes first processing means, first storage means, and a timer; (*US '323: see column 2, line 44*)

a base computing system including second processing means and second storage means; (*see column 2, line 45*)

a connection between said portable computing system and said base computing system for transmitting data between said portable computing system and said base computing system; (*see column 2, line 47*) and

a first program, executing within said first processing means, causing said portable computing system to perform a process including:

determining if a public cryptographic key is stored in a first location within said first storage means;

in response to determining that a public cryptographic key is not stored in said first location, transmitting a request code, receiving said public cryptographic key, and storing said public cryptographic key in said first location; (*see column 3, lines 42 – 51*)

transmitting a first code;

receiving a response to said first code;

determining from said response to said first code if a connection has been made to said base computing system; and (*see column 3, lines 23 – 24*)

and

a second program, executing within said second processing means, causing said base computing system to perform a process including:

receiving said request code; in response to receiving said request code, transmitting a public cryptographic key of said base computing system to said portable computing system;

receiving said first code; and

in response to receiving said first code, transmitting said response to said first code (*US '323: see column 3, lines 52 – 58*)

but does not teach

setting said timer to run until said specified time has expired; a subroutine executing within said first processing means, causing said portable computing system to perform a process including:

determining if said timer is running; and

providing access to said secure data only when said timer is running.

Godoroja et al. in US '258 however does teach

setting said timer to run until said specified time has expired; a subroutine executing within said first processing means, causing said portable computing system to perform a process including:

determining if said timer is running; and

providing access to said secure data only when said timer is running; (*US '258: see column 3. lines 23 – 24 and column 5, lines 58 – 65*).

For claim 16, *it would be obvious to one of ordinary skill in the art at the time of the invention to modify the methods of Godoroja et al. and Shimizu et al. as they both use features of a portable and base computing systems and timer functionalities within the same field of endeavor (connecting to and accessing secure data during specified time) and with the same problem sought to be solved (providing controlled access to secure data within specific time).*

For claim 17, *Godoroja et al. shows* wherein

said first storage means includes a timer register storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register (*US '258: see column 4, lines 61 – 65).*

For claim 18, *Shimizu et al. shows* wherein

said step of transmitting a first code includes generating a random number, storing said random number in a second location within said first storage, and transmitting said random number to said base computing system as said first code, (*US '323: see column 4, lines 21 – 23*)

said step of transmitting said response to said first code includes encrypting said random number with a private cryptographic key of said base computing system to form an encrypted random number, and transmitting said encrypted random number as said response to said portable computing system as said response to said first code, (*US '323: see column 4, lines 24 – 28*) and

said step of determining from said response to said first code if a connection has been made to said base computing system includes decrypting said encrypted number to form a decrypted number and comparing said decrypted number with said random number stored in said second location within said first storage (*US '323: see column 4, lines 29 – 33).*

For claim 19, *Shimizu et al. shows* wherein

said first processing means includes a first microprocessor and a first cryptographic processor,

said encrypted number is decrypted in said first cryptographic processor,

said first storage means includes first secure storage accessed only through said first cryptographic processor, and

said first location and said timer register within said first storage means are within said secure storage (*US '323: see Figure 10 – 11 and column 12, lines 4 – 15: where it is inherent that there is a cryptographic processor within each information processing apparatus).*

For claim 20, *Shimizu et al. shows* wherein

said second processing means includes a second microprocessor and a second cryptographic processor,

said random number is encrypted to form said encrypted number within said second cryptographic processor,

said second storage means includes second secure storage accessed only through said second cryptographic processor, and

said private cryptographic key of said base computing system is stored within said second secure storage (*US '323: see Figure 10 – 11 and column 12, lines 4 – 15).*

For claim 21, *Shimizu et al. in US '323 teaches*

said portable computing system additionally includes a display,

said first program additionally causes a successful completion message to be displayed on said display in response to a determination from said response to said first

code that a connection has been made to said base computing system, and (*US '323: see Figure 8 and Figure 12)*

but does not show

said first program additionally causes an error message to be displayed on said display in response to a determination from said response to said first code that a connection has not been made to said base computing system.

Godoroja et al. in US '258 however does teach

said first program additionally causes an error message to be displayed on said display in response to a determination from said response to said first code that a connection has not been made to said base computing system *(US '258: column 3, lines 2 – 3: where the header includes information about transmission).*

For claim 21, *it would be obvious to one of ordinary skill in the art at the time of the invention to combine the methods of Godoroja et al. and Shimizu et al. as they both use features of a portable and base computing systems and timer functionalities within the same field of endeavor (displaying message based on connection between computing systems) and with the same problem sought to be solved (providing controlled access to secure data within specific time).*

For claim 22, *Shimizu et al. teaches*

said portable computing system additionally includes a display and a keyboard, and

said first program causes said portable computing to perform a process additionally including displaying a menu, receiving a user input from said keyboard as

said menu is displayed, and determining said specified time from said user input *(US '323: see Figure 12)*.

For claim 23, *Shimizu et al. teaches*

said portable computing system additionally includes a display and a keyboard,

said first program causes said portable computing to perform a process additionally including displaying a menu and receiving a password from said keyboard as said menu is displayed,

said step of transmitting a first code includes:

generating a random number;

storing said random number in a second location within said first storage; (*US '323: see Figure 8: as performed by the temporary key generator*) *and*

encrypting said concatenated number with a private cryptographic key of said portable computer system stored in a third location within said first storage means to form said first code; and

transmitting said random number to said base computing system as said first code,

said step of transmitting said response to said first code includes:

decrypting said first code with a private cryptographic key of said base computing stored in a fourth location within said second storage means;

separating said password from said random number;

determining whether said password separated from said random number matches a password stored;

encrypting said random number with a private cryptographic key of said base computing system to form an encrypted random number, and

determining if and transmitting said encrypted random number as said response to said portable computing system as said response to said first code, said second program causes said base computing system to perform a process additionally including:

determining if a password is stored in a fifth location within said second storage means;

in response to a determination that a password is not stored in said fifth location, storing said password separated from said random number in said fifth location;

in response to a determination that a password is stored in said fifth location, comparing said password stored in said fifth location with said password separated from said random number;

in response to determining that said password stored in said fifth location matches said password separated from said random number, encrypting said random number and to form a transmitting an approval code to said portable computing system as said response to said first code; and

said step of determining from said response to said first code if a connection has been made to said base computing system includes determining that said approval code has been received

but does not teach

concatenating said random number with said password to form a concatenated number.

Godoroja et al. in US '258 however does teach

concatenating said random number with said password to form a concatenated number *(US '258: column 3, lines 54 – 59: combining said characteristics) as taught by*

For claim 23, *it would be obvious to one of ordinary skill in the art at the time of the invention to combine the methods of Godoroja et al. and Shimizu et al. as they both use features of a portable and base computing systems and timer functionalities within the same field of endeavor (arranging values in such a way as to create a value to compare before data is exchanged) and with the same problem sought to be solved (providing controlled access to secure data within specific time).*

For claim 24, *Godoroja et al. in US '258 shows* wherein

said second program causes said base computing system to perform a process additionally including, in response to determining that said password stored in said fifth location does not match said password separated from said random number, transmitting an error code to said portable computing system as said response to said first code

said first program causes said portable computing to perform a process additionally including displaying a successful completion message on said display in response to receiving said approval code, and displaying an error message on said display in response to receiving said error code (*US '258: see column 3, lines 2 – 3*).

For claim 25, *Godoroja et al. in US '258 shows* wherein

said first storage means includes a timer register storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register (*US '258: see column 4, lines 61 – 65)*.

For claim 26, *Shimizu et al. shows* wherein

said first processing means includes a first microprocessor and a first cryptographic processor,

said concatenated number is encrypted in said first cryptographic processor,

said first storage means includes first secure storage accessed only through said first cryptographic processor, and

said secure storage includes said first location, said third location, and said timer register within said first storage means (*US '323: see Figure 10 – 11 and column 12, lines 4 – 15)*.

For claim 27, *Shimizu et al. shows* wherein

said second processing means includes a second microprocessor and a second cryptographic processor,

said random number is encrypted to form said encrypted number within said second cryptographic processor,

said second storage means includes second secure storage accessed only through said second cryptographic processor, and

said fourth and fifth locations within said second storage means are within said second secure storage (*US '323: see Figure 10 – 11 and column 12, lines 4 – 15).*

For claim 28, *Shimizu et al. shows*

said step of transmitting a request code includes transmitting a public cryptographic key of said portable computing system, and

said step of receiving a request code includes storing said public cryptographic key of said portable computing system in a sixth location within said second storage means *(US '323: see Figure 10 – 11 and column 12, lines 4 – 15)l.*

For claim 29, *Shimizu et al. in US '323 teaches*

A computer readable medium within a portable computing system, wherein said computer readable medium has computer readable instructions for performing a method comprising:

determining if a public cryptographic key is stored in a first location within said first storage means;

in response to determining that a public cryptographic key is not stored in said first location, transmitting a request code, receiving said public cryptographic key, and storing said public cryptographic key in said first location;

transmitting a first code;

receiving a response to said first code;

determining from said response to said first code if a connection has been made to a base computing system; (*US '323: see column 3, lines 42 –51*) and

but does not teach

setting a timer to run until a specified time has expired.

Godoroja et al. in US '258 however does teach

setting a timer to run until a specified time has expired (*US '258: see column 5, lines 58 – 65*) *as taught by Godoroja*.

For claims 29, *it would be obvious to one of ordinary skill in the art at the time of the invention to combine the methods of Godoroja et al. and Shimizu et al. as they both use features of a portable and base computing systems and timer functionalities within the same field of endeavor (exchanging data with a specified time period) and with the same problem sought to be solved (confirming users and connections between systems).*

For claim 30, *Godoroja et al. teaches*

wherein said step of setting aid timer includes storing a number corresponding to said specified time in a timer register (*US '258: see column 4, line 61 – 65*).

For claim 31, *Shimizu et al. teaches*

said step of transmitting a first code includes generating and storing a random number, and transmitting said random number to said base computing system as said first code, and

said step of determining from said response to said first code if a connection has been made to a base computing system includes decrypting an encrypted number to form a decrypted number and comparing said decrypted number with said random number (*US '323: see column 4, lines 21 – 28*).

For claim 32, *Godoroja et al. teaches*

displaying a successful completion message in response to receiving an approval code; and

displaying an error message in response to receiving an error code (*US '258: see column 3, lines 2 – 3*).

For claim 33, *Shimizu et al. teaches*

displaying a menu;

receiving an input from a keyboard as said menu is displayed; and

determining said specified time from said input (*US '323: see Figure 12, item 22; and column 14, lines 15 - 26*).

For claim 34, *Shimizu et al. in US '323 teaches*

The computer readable medium of claim 29, wherein said method additionally includes displaying a menu and receiving a password from a keyboard as said menu is displayed, said step of transmitting a first code includes:

generating a random number;

storing said random number in a second location within said first storage;

and

encrypting said concatenated number with a private cryptographic key of said portable computer system stored in a third location within said first storage means to form said first code; and

transmitting said random number to said base computing system as said first code (*US '323: see Figure 8: temporary key generator; and column 10, lines 58 – column 11, lines 1 – 10*)

but does not teach

concatenating said random number with said password to form a concatenated number.

Godoroja et al. in US '258 however does teach

concatenating said random number with said password to form a concatenated number, (*US '258: column 3, lines 54 – 59*).

For claims 34, *it would be obvious to one of ordinary skill in the art at the time of the invention to combine the methods of Godoroja et al. and Shimizu et al. as they both use features of a portable and base computing systems and timer functionalities within the same field of endeavor (arranging values in such a way as to create a value to compare before data is exchanged) and with the same problem sought to be solved (providing controlled access to secure data within specific time).*

For claim 35, *Shimizu et al. in US '323 teaches*

In a portable computing system having a user interface including a display and a

keyboard, a method for limiting access to secure data to a specified time, wherein said method comprises:

displaying a screen location for entering a number;

accepting an input from said keyboard;

displaying said input from said keyboard in said screen location;

calculating a number determining said specified time as a function of said input from said keyboard; (*US '323: see Figure 12 and column 14, lines 15 – 26)*

generating a random number;

transmitting said random number to a base computing system;

receiving an encrypted number from said base computing system,

decrypting said encrypted number with a public cryptographic key stored within said portable computing system to form a decrypted number;

determining if said random number matches said decrypted number; and

in response to determining that said random number matches said decrypted number, (*US '323: see Figure 8 and column 13, lines 38 – 40*)

but does not teach

setting a timer within said portable computing system to run for said specified time, wherein said access to secure data is provided only when said time is running (*US '258 column 3, lines 23 – 24 and column 5 lines 58 – 65).*

For claim 36, *Godoroja et al. teaches*

displaying a successful completion message in response to determining that said random number matches said decrypted number; and

displaying an error message in response to determining that said random number does not match said decrypted number (*US '258: see column 3, lines 2 – 3).*

For claim 35, *it would be obvious to one of ordinary skill in the art at the time of the invention to combine the methods of Godoroja et al. and Shimizu et al. as they both use features of a portable and base computing systems and timer functionalities within the same field of endeavor (displaying message based on connection between computing systems) and with the same problem sought to be solved (limiting access to secure data within a specified time).*

For claim 37, *Shimizu et al. in US '323 teaches*

In a portable computing system having a user interface including a display and a keyboard, a method for limiting access to secure data to a specified time, wherein said method comprises:

displaying a first screen location for entering a password and a second screen location for entering a number;

accepting a first input from said keyboard;

generating a password from said first input;

accepting a second input from said keyboard;

displaying said input from said keyboard in said second screen location;

calculating a number determining said specified time as a function of said second input from said keyboard; (*US '323: see Figure 12 and column 14, lines 15 – 26)*

generating a random number;

encrypting said password with a public cryptographic key stored in said portable computing system;

transmitting said random number to a base computing system;

receiving an encrypted number from said base computing system,

decrypting said encrypted number with said public cryptographic key stored within said portable computing system to form a decrypted number;

determining if said random number matches said decrypted number; and in response to determining that said random number matches said decrypted number, (*US '323: see Figure 8 and column 13, lines 38 – 40*)

but does not teach

setting a timer within said portable computing system to run for said specified time, wherein said access to secure data is provided only when said time is running.

Godoroja et al. in US '258 however does teach

setting a timer within said portable computing system to run for said specified time, wherein said access to secure data is provided only when said time is running (*US '258 column 3, lines 23 – 24 and column 5 lines 58 – 65).*

For claim 37, *it would be obvious to one of ordinary skill in the art at the time of the invention to combine the methods of Godoroja et al. and Shimizu et al. as they both use features of a portable and base computing systems and timer functionalities within the same field of endeavor (displaying message based on connection between computing systems) and with the same problem sought to be solved (limiting access to secure data within a specified time).*

For claim 38, *Godoroja et al. teaches*

displaying a successful completion message in response to determining that said random number matches said decrypted number; and

displaying an error message in response to determining that said random number does not match said decrypted number and in response to receiving an error code from said base system (*US '258: see column 3, lines 2 – 3).*

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Teraoka in US 6009528 A discloses ideas parallel to applicant's claimed invention.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurel Lashley whose telephone number is 571-272-0693. The examiner can normally be reached on 7:30 am - 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Laurel Lashley
Examiner
Art Unit 2132

September 30, 2005
LLL

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100